3.1 DoS/DDoS攻撃対策(1) ～ISPにおけるDDoS対策の現状と課題～

齋藤　衛（(株)インターネットイニシアティブ）

ISPとDDoS攻撃

DDoS（Distributed Denial of Service）攻撃は，特定組織の通信の機能を麻痺させ，インターネット上から消え失せたように見せることを最終的な目的とする威力行為で，その組織のインターネット接続回線やサーバなどの，有限の通信資源に対して輻輳を発生させる．インターネットサービスプロバイダ（以降，ISP）の立場では，攻撃を受けたユーザからの申告により攻撃への対処を行う場合には，ユーザと相談の上，その攻撃の種類や規模に応じた対応を行うことがある．DDoS攻撃対策を行うサービスは，国内においては2005年より登場しており，ユーザはこれらのサービスを利用して攻撃への対策を実施できるようになっている．

また，通信事業は，もとより有限の通信資源を用意し，それをユーザに提供していることで成立する設備中心の産業であると考えることができる．資源の総量は，ユーザの通常の利用量とその予測から計画的に配置される．このため，通信サービスを提供するISPの立場では，DDoS攻撃による異常な通信の集中を緩和することで，通信資源を保護したり，自社のサービスの安定的提供を継続することを主眼に，正当防衛もしくは緊急避難として恣意的に攻撃の通信に対処したりすることもある．

一方で，DDoS攻撃が発生したときに，たとえばISPとユーザの間の回線が埋まってしまうような大規模な攻撃の場合，ユーザ側では攻撃トラフィックの総量を把握できず，ユーザ側の情報だけでは適切な対策を立案できない可能性がある．この事実だけでも，DDoS攻撃への対策はISPとユーザが連携し協議の上で実施すべきものであると言うことができる．

本稿では，日本国内におけるDDoS攻撃とその対策の状況と，これから解決すべき課題について紹介する．

日本におけるDDoS攻撃の変遷

まず，日本において発生したDDoS攻撃の状況について述べる．

■ DDoS攻撃の発生理由

インターネット上では，1990年代から，ネットワークワームやメールウイルスの感染活動の際に発生させる大量通信により，サーバや回線への過負荷など，DDoS攻撃に似た事象が発生していた．2000年ごろには専用のDDoS攻撃ツールが登場し，特に米国において有名サイトなどに対するDDoS攻撃が起きている．筆者が国内で最初に対応したDDoS攻撃は2003年5月に発生した，過激な動物愛護団体による動物実験への抗議活動としての攻撃であった．その後2005年ごろからは，さまざまな理由で発生するDDoS攻撃に日常的に対応するようになった（図-1）．

また，国外では，政変や戦争などの実社会での事変に乗じて，インターネット上で同時にDDoS攻撃が行われることも増えてきている．ここまでは日本国内の組織が被害者となった例を紹介してきたが，その一方で，多量の接続を繰り返し誘発するスクリプトなどを用いて，攻撃者となるユーザが国内にも存在している状況がある．

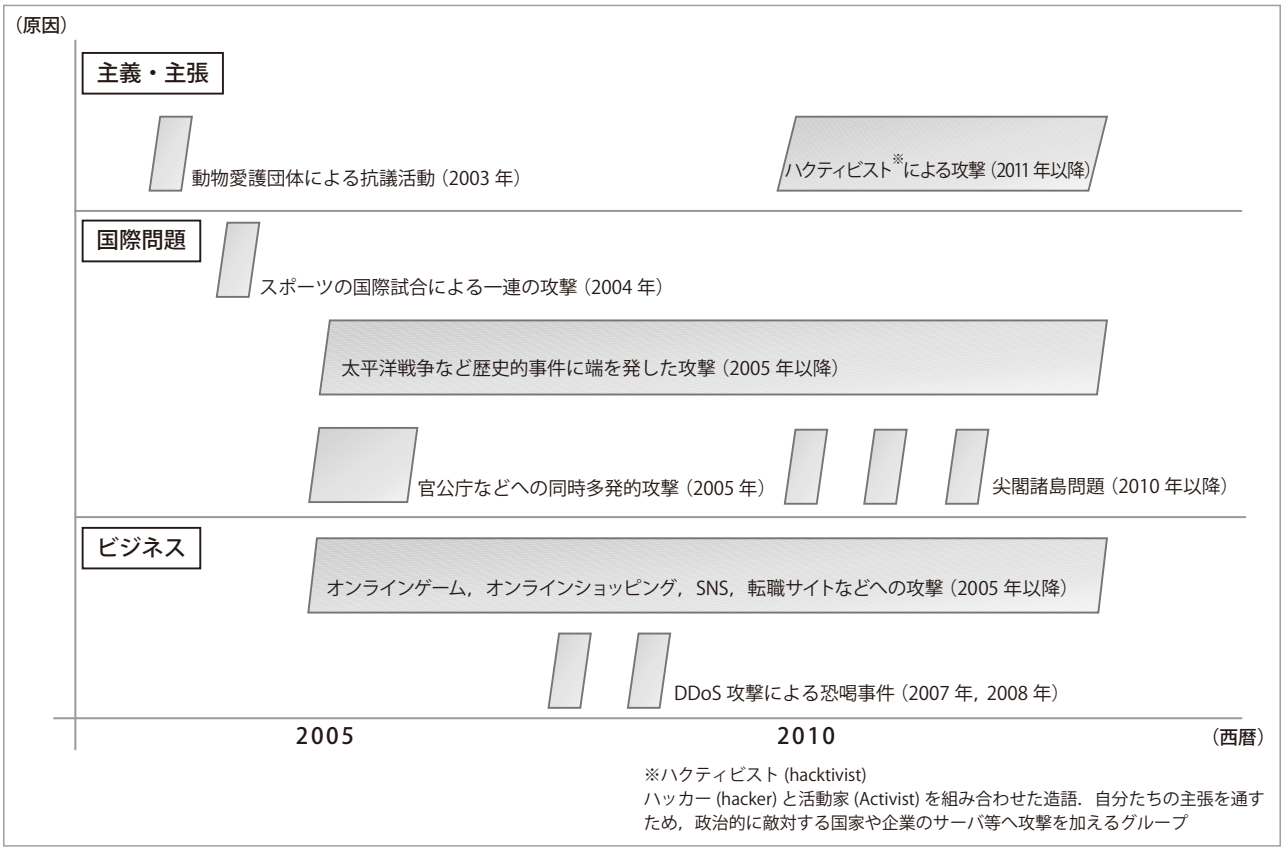

図 -1　国内における DDoS 攻撃の発生原因の推移

■ DDoS 攻撃の攻撃対象

一般には Web サーバに対する DDoS 攻撃がよく話題となるが，攻撃対象となった組織のサイト上のすべてのシステム，たとえば，メールサーバや DNS サーバなども攻撃対象となることが多い．これらのサーバでは，蓄積型の通信やキャッシュの仕組みによって，Web サーバよりも攻撃の影響が表面化しにくい．しかし，攻撃による影響が長期化した場合には，広範囲に深刻な影響を及ぼすことになる．このように DDoS 攻撃は，Web サーバだけの問題ではなく，インターネットに露出したサイト上のシステムはそれがどんなシステムであっても DDoS 攻撃に対する備えを行うべきである．

■ DDoS 攻撃の発生件数と攻撃規模の変遷

ここで，筆者の所属する ISP における DDoS 対策サービスで取り扱った DDoS 攻撃対処件数の推移を図 -2 に示す．

この情報は，定期刊行している技術レポート [1] に掲載してきた 2008 年 9 月からの情報を 1 つにまとめたものである．ここでは，攻撃対象に着目して，サーバを過負荷にすることを目的とした攻撃（TCP SYN Flood 攻撃や TCP Connection Flood 攻撃など），回線容量を埋めようとする攻撃（UDP Flood 攻撃など），その両者の複合的な攻撃の 3 種類に分類している．攻撃の規模は，たとえば回線に対する攻撃の場合，10 年前は数百 Mbps 規模であったものが，2012 年には国内でも 10Gbps を超える攻撃が観測されている．また，国外，特に米国においては 70Gbps を観測するなど，インターネット利用環境の拡充整備に伴い，DDoS 攻撃の規模も徐々に大きくなっている様子がうかがえる．

ISP による DDoS 攻撃対策

以上のような状況に対し，ISP で実際に行われている DDoS 対策について紹介する．

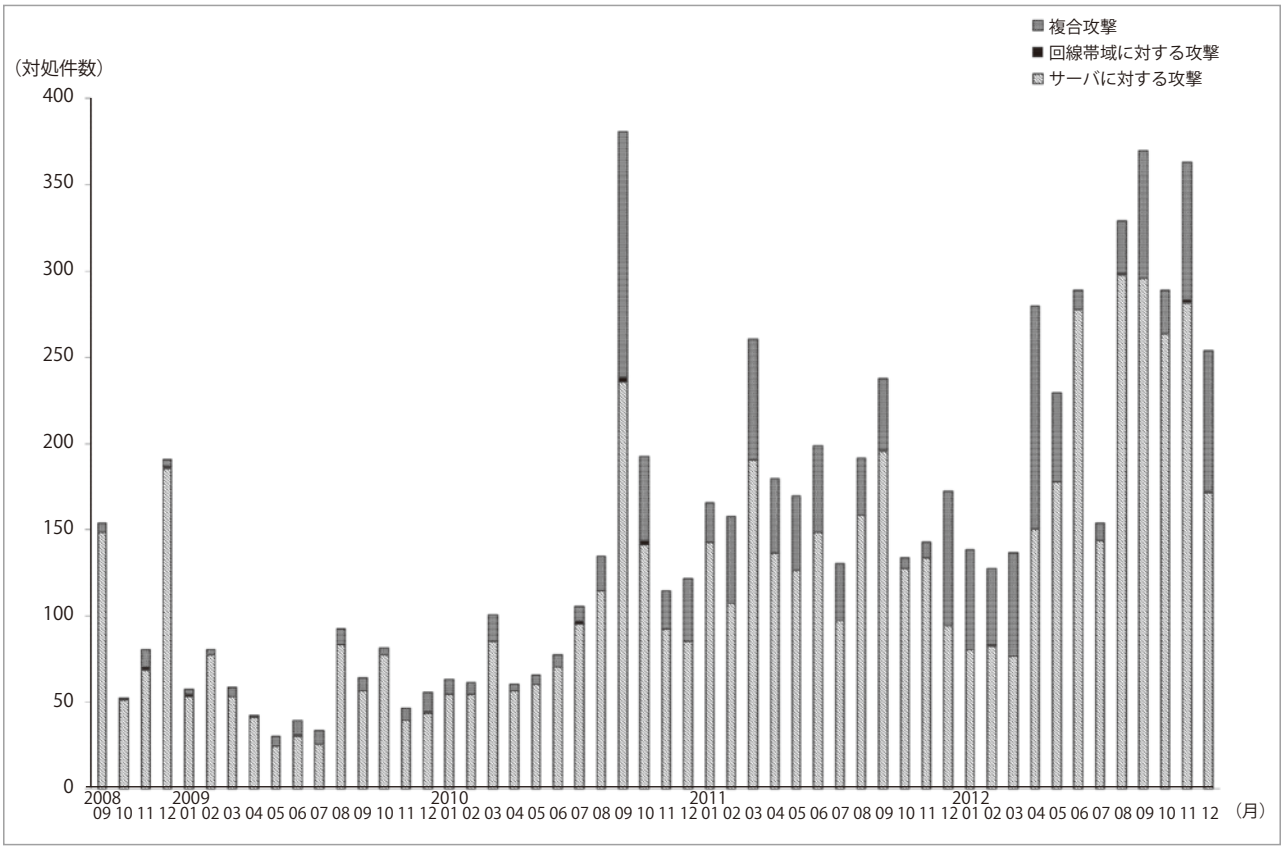

図 -2　インターネットイニシアティブ（IIJ）が DDoS 対策サービスで対処した攻撃の推移

■ DDoS 攻撃の観測

DDoS 攻撃は，特定の組織を狙った忌避行為であり，被害者をインターネット上から排除することを目的としている．このため，インターネット上で発生する事件としては珍しく，攻撃者と被害者が明確であることが多い．したがって，過去の攻撃の事例や一般ニュースなどから動静情報を調査し，攻撃予告や攻撃発生の予兆を把握することも，重要な対策の 1 つとなっている．

同様に，バックスキャッタ観測☆1 により，第三者に対して発生している DDoS 攻撃の一部を観測するなど，世界的な発生状況を把握しておくことも，日本に対して発生する攻撃を予測する意味で役に立つ．さらに，DDoS 攻撃に利用される攻撃ツールやマルウェアなどの解析情報も，攻撃の種類や規模を予測するために活用している．

これらの情報は ISP で個別に収集・解析を実施しているが，国内における同時多発的な攻撃の発生時などでは，テレコム・アイザック推進会議（以降，Telecom-ISAC Japan）などの業界団体を中心に，複数の ISP の間で活発に情報交換が行われている．

■ DDoS 対策装置による防御

次に，多くの ISP で提供している DDoS 攻撃対策のサービスについて説明する．これらのサービスでは，専用の DDoS 対策装置が用いられていることが多い．現在では，このような装置にも複数の製品が存在し，その対応する攻撃の種類や規模などで一長一短がある．また，多くの装置において，その基本機能として，異常検知，代理応答，攻撃通信に対する操作の 3 つの機能を提供している．

異常検知

異常検知の機能は，通信の総量や TCP 接続量，アプリケーションプロトコルごとなどの通信量につ

☆1 バックスキャッタとは，攻撃の通信に応じて被攻撃サーバが送出する応答（TCP SYN/ACK パケットなど）のこと．発信元 IP アドレスが詐称されている場合には，詐称に使われた発信元 IP アドレスに応答パケットが送信されることから，このパケットを捕捉することにより，発生している DDoS 攻撃の一部を観測できる．

いて異常を判定し，攻撃を検出する機能である．時系列の統計モデルにより正常な状態を定義し，その状態からの逸脱を異常として検出することが多い．通信の観測点としては，ユーザのサーバの通信を直接観測する場合や，ISP のバックボーンで取得されるサンプリングされた NetFlow[2] のデータを利用する場合などがある．

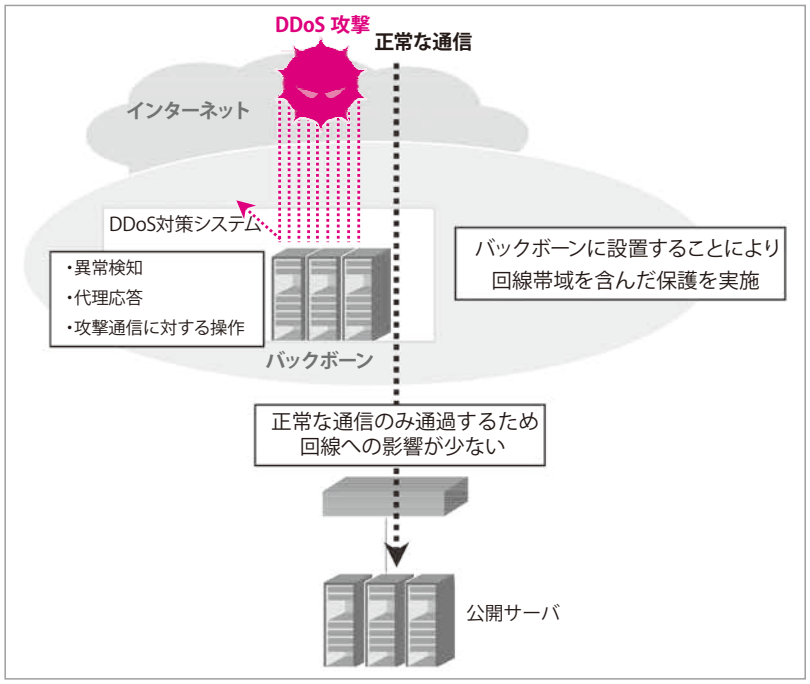

図 -3　ISP による DDoS 対策サービスの概要

代理応答

代理応答の機能は，DDoS 攻撃ツールの多くが通信プロトコルに従わないという特徴を利用して，攻撃通信か否かを見分ける機能である．この機能の場合，攻撃者と被害者の間に設置した DDoS 対策装置が，攻撃者からの要求に被害者に代わって応答をする．対策装置の送信した応答に，通信プロトコルに則って呼応してくる通信を正当な通信と判断し，その通信のみを保護対象に送ることで，攻撃の通信トラフィックが被害者に到達することを防いでいる．また，TCP SYN Flood 攻撃などの通信プロトコルの低レイヤを利用した DDoS 攻撃の場合には，発信元 IP アドレスが詐称されていることが多く，この機能を利用することで攻撃通信の発信者が実際に存在するか否かを見分けることができる．

攻撃通信に対する操作

攻撃通信に対する操作としては，単純な IP アドレスによるアクセス制御や，IP アドレスごとやプロトコルごとに設定される帯域制御などが挙げられる．

以上のような機能を備えた装置を ISP のネットワーク上に配備し，ユーザに向かった通信の異常を排除することで，ユーザの回線とサーバを保護するのが ISP における DDoS 攻撃対策のサービスである（図 -3）．

■ サーバ側での対策

DDoS 攻撃では，攻撃の量が一定であったとしても，攻撃を受けるサーバの処理能力に依存してその影響が大きく変化する．このため，攻撃を受ける可能性のあるサーバについては，事前に DDoS 攻撃への耐性をつけることを推奨している．

たとえば，サーバで利用する OS の多くには，すでに TCP SYN Flood 攻撃に対する代理応答の機能や，発信元 IP アドレスごとやアプリケーションごとに接続数を制限する機能が内蔵されている．これらを適切に設定しておくことで，攻撃による影響をある程度緩和できる．同時に，アプリケーションのサーバ実装において，同時接続数の制限や処理の上限を設定すること，負荷分散装置の機能を有効に活用することも検討すべきである．

また，サーバにおける日常的な運用においてログを取得，解析，精査し，正常な通信量の範囲を把握しておくことで，攻撃の発生を早期に発見することができるようになる．

■ ネットワーク技術による対策

ISP によっては，ネットワーク上の通信の制御技術を駆使して DDoS 攻撃対策を実施することもある．

まず，ネットワークを構成するルータによるアクセス制御や，経路による攻撃通信トラフィックの吸い込み（Blackholing[☆2]）が挙げられる．このとき，

実装などの制約から，攻撃元となる発信元 IP アドレスで制御できる場合はまれであり，通常は被害を受けているユーザに向けた通信をすべて破棄することになる．

また，ユーザがサーバ類を複数のクラウドやデータセンタなどに分散配置しているような場合には，通信の分散技術や，IP の Anycast[3), 4)] などの経路技術と組み合わせて対策を実施することができる．この際には，攻撃の通信トラフィックを分散させたり，攻撃者に近い拠点に集中させたりするとともに，他の拠点に設置したサーバを用いてユーザへのサービスを継続する（図 -4）．

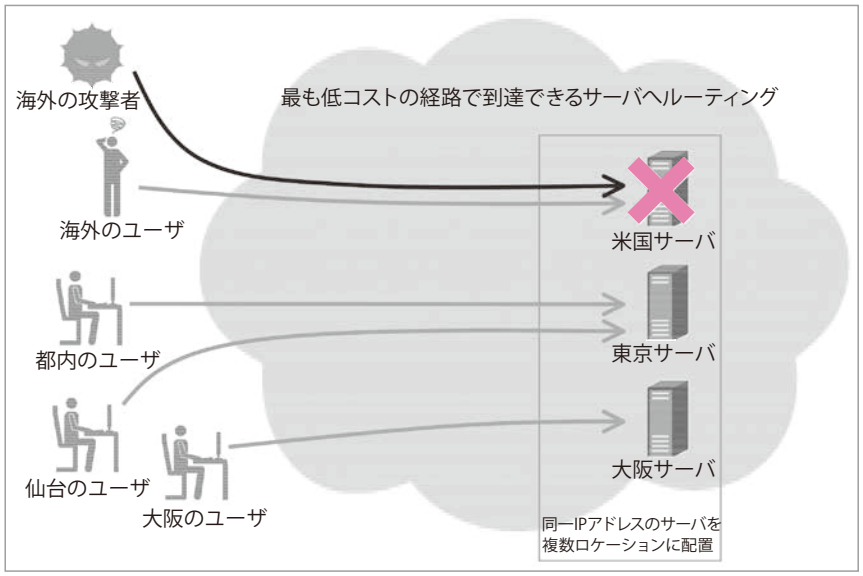

図 -4　ネットワーク技術による DDoS 攻撃対策（IP Anycast の例）

この手法には，経路操作を必要とするため，ネットワークを運用する ISP やデータセンタ事業者などの通信事業者との協力や，ユーザが経路制御などの通信の機能を持った上で実施することになる．このため，それ相応の設備や設定，運用を行う必要があり，全体のコストで見れば現状ユーザにとって高価な対策となっている．

■ ISP による DDoS 攻撃対策のためのガイドライン

これまで紹介してきたような対策は，通信状況の把握と通信に対する操作が主である．このような対策を通信主体であるユーザではなく，ISP が実施することは電気通信事業法上の通信の秘密を侵害する行為である．このため，ISP が対策を躊躇したり，対策の判断に時間を要したりする場合がある．

そこで，迷惑メールや DDoS 攻撃など大量の通信を伴う現象について，個々の ISP が状況に応じた適切な対策を実施できるように，技術詳細と適用条件，その例をまとめたものが「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」[5)] である．このガイドラインは 2007 年に策定され，2011 年 3 月に改訂と一般公開されており，国内 ISP はこれを参照して対策を検討している（図 -5）．

このガイドラインの事例の多くは，ユーザからの依頼を契機とした調査や対処について記載されている．ISP の独自の判断による対処は，通信設備保護のための正当防衛などの場合のみ許される．ただし，このガイドラインに記載してあるからといって ISP が必ずその対応を実施するとは限らない．個別事案の実際の状況に応じて，対応コストや事業法違反とならないかどうかの判断を行い，最終的にはユーザや監督官庁などとの協議の上に対策を実施することになる．

■ DDoS 対策の限界と副作用

ISP において DDoS 対策を実施する理由としては，ユーザのシステム保護と，自社の通信資源保護の 2 つがある．ここでは，この 2 つに適用される技術の限界，結果の違いについて述べる．

ユーザのシステム保護

まず，DDoS 攻撃に備えていないサーバは，あまり適切に保護することができない．攻撃対象のサーバの限界が低い場合には，DDoS 対策装置の異常判

☆2 Blackholing：ルータで攻撃パケットを破棄する方法で，攻撃通信のパケットを廃棄するルータをあらかじめ決定し，そのルータ上で破棄する IP アドレスの経路の次ホップを Null 0（廃棄）に向けて設定する．アクセス制御などと異なり，経路制御とパケット転送のエンジンを用いて実現するため，多くのルータ実装において負荷をかけずに高速に実施することができる．

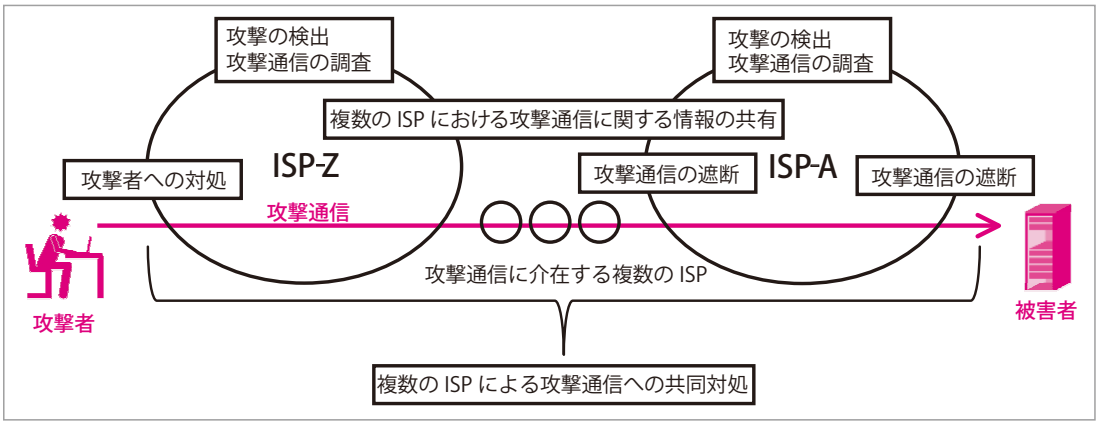

図 -5
ガイドライン中の
DDoS 攻撃対策

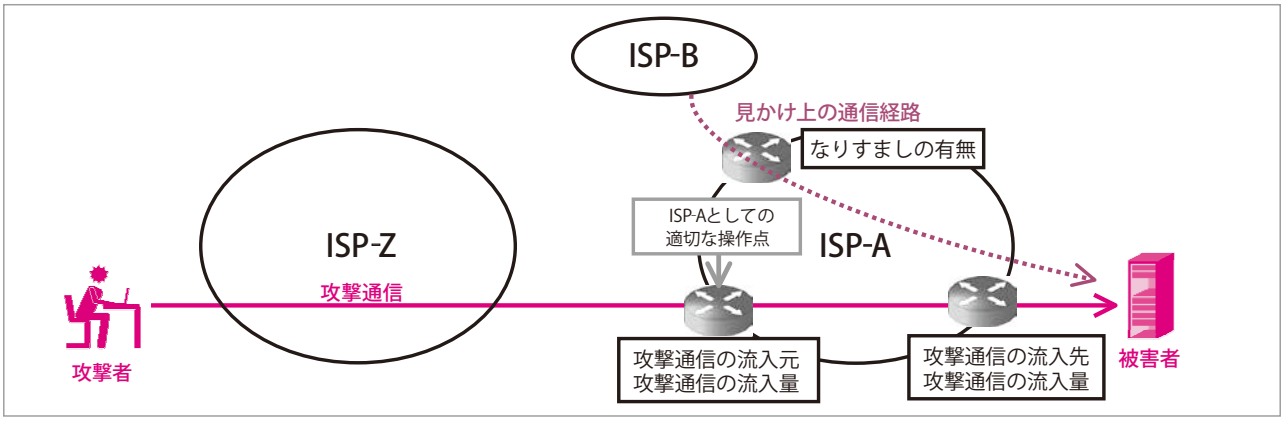

図 -6　ISP の把握する DDoS 攻撃の様子と操作点

定において少ない通信量の正常な通信を攻撃とする誤判断が起こる可能性がある．逆に，DDoS 対策装置が正常と判断して通過させた通信だけで，影響を受けることも起こる．このように，DDoS 攻撃を受けたシステムが上述で示したような『サーバでの対策』を実施していない場合には，DDoS 対策装置導入による対策効果がなくなる可能性がある．

また，ユーザから申告があった場合でも，ISP のバックボーン上では，通信量の少ない攻撃については，その異常の発生や流入元を把握できないことがある．この場合，攻撃対象となったサーバのログから対策を検討するが，そのための通信記録を保持していない場合，攻撃の概要すら把握できなくなる．このように，ユーザ自身が DDoS 攻撃に備える努力を行うことが必要となる．

自社の通信資源の保護

次に，ISP の判断で対策を実施する場合について述べる．DDoS 対策装置の処理能力を大きく上回るような攻撃の場合，もしくは ISP 自身の通信設備が攻撃対象となった場合には，上述の『ネットワーク技術による対策』を駆使した対策を実施することがある．この場合においては通信を操作する場所により，その影響範囲が異なってくる．

たとえば，図 -6 の ISP-A において，網内の ISP-Z との接続点で攻撃の通信をアクセス制御で排除したとする．このとき，ISP-A の通信資源は保護されるが，ISP-Z に属する一般の利用者は，被害者に対する通信ができない状況が発生する．被害者にとっては，通信機会の大きな損失となりかねない．このため，ISP の判断による対策についても，基本的にはユーザと協議の上で実施することが多い．

さらに，サーバを複数のデータセンタに分散して配備した場合でも，結果として攻撃者に近いサーバは過負荷になったり，サービスが継続できなくなったりし，インターネット上の特定の範囲から一般の利用者がアクセスできなくなる場合が想定される．加えて，これまで紹介してきた DDoS 攻撃対策手法のうちのいくつかは，対策手法そのものが悪用さ

れてしまうことにより，保護すべきサイトへの通信を阻害したり，ほかの DDoS 攻撃に転用されてしまったりする可能性がある．このため，その適用と運用に十分な注意が必要となる．

以上のように DDoS 攻撃対策には副作用と限界があり，攻撃手法と攻撃の規模，攻撃対象の状況によって適切な対策が異なる．また，その対策の結果としてユーザの立場で許容できる状況と，ISP が実施できる対策の間に差異が生まれることがある．たとえば 2004 年に発生したマルウェア Antinny によるコンピュータソフトウェア著作権協会（ACCS）の Web サーバへの DDoS 攻撃の場合，ISP の立場では共同対処により，不要な大量通信を排除することに成功した．一方，ACCS の立場では，対処中も Web サーバでの情報発信は停止したままであった．これはユーザの立場では，本来望む状況ではない☆3．ほかの攻撃の対策事例の場合には，対処により通信機会の損失が発生することを懸念したユーザの判断で，ISP における対策を実施しなかったケースもある．

DDoS 攻撃対策の課題

最後に，これまで紹介してきた DDoS 対策を，より良いものにしていくための課題提起をしたい．

2009 年 7 月韓国で，大規模かつ連続的な DDoS 攻撃事案が発生した[6]．この事案では，マルウェアに感染した韓国国内 10 万台規模の PC が，攻撃者の命令に応じて当初は米国のサーバを，後に韓国国内のサーバを攻撃し続け，国民生活に影響を与えたことで大きな問題となった．日本においてもこのような事件が発生したとすると，国内 ISP のユーザ同士で互いに攻撃しあうような状況が，より大規模に発生することが想定される．

このような状況に対しては，これまで紹介してきた対策だけでは解決することのできない次のような課題がある．

1）ユーザから DDoS 攻撃が発生した場合の検出および対処について十分な検討がなされていない．
2）対応時間の短縮化，特に自動化について，複数の ISP が協力する手法が確立されていない．
3）各 ISP が独自判断で対策を実施することにより，日本のインターネットを分断するようなことにならないための協調の場が構築されていない．

これらのうち 1）と 2）については，国外クラウド事業者のユーザが DDoS 攻撃を発生させた場合の対応状況や，ISP のコミュニティにおける協調対処など，先行する試みがいくつか存在する．そこで用いられているプロトコルや実装，つまり既存の技術を適用することが可能だと考えらえる．しかし，適法性やコストなどの現実的な制約のもとで，国内 ISP が無理なく実践できることを目指して検討しなければならない．

最後の課題については，たとえば韓国の例のように政府主導で法的な裏付けと責任をもって統制するということも考えらえる．しかし，日本においては，ISP のコミュニティが，個別ユーザや ISP の状況を把握し，日本全体を見渡す視点を持ち，場合によっては対処の判断ができる能力を持つことが現実的な第一歩であると考えている．

これらの課題を解決するために，Telecom-ISAC Japan の DoS 攻撃即応ワーキンググループにおいて検討を重ね，複数の ISP が協調対処を行うことのできる関係構築に向けた努力を実施している．

☆3 ACCS の Web サーバへの DoS 攻撃については，本特集の「2.2 DoS/DDoS 攻撃観察日記 (2)」も参照のこと．

参考文献

1) IIJ : Internet Infrastructure Review (IIR), http://www.iij.ad.jp/company/development/report/iir/index.html
2) IETF : RFC3954 Cisco Systems NetFlow Services Export Version 9, http://www.ietf.org/rfc/rfc3954.txt
3) IETF : RFC4768 Operation of Anycast Services, http://www.ietf.org/rfc/rfc4786.txt
4) IIJ : 松崎吉伸 : d.dns.jp の運用，http://www.iij.ad.jp/company/development/tech/activities/ddnsjp/index.html
5) インターネットの安定的な運用に関する協議会 : 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドラインの改定について，http://www.jaipa.or.jp/topics/?p=400
6) IIJ : Internet Infrastructure Review (IIR) Vol.5「1.4.1 米国および韓国における DDoS 攻撃」, http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol05.pdf

(2013 年 2 月 18 日受付)

■齋藤　衛　msaito@iij.ad.jp

（株）インターネットイニシアティブ サービスオペレーション本部 セキュリティ情報統括室 室長．Telecom-ISAC Japan 運営委員，DoS 攻撃即応ワーキンググループ主査．